2023.04.28

IOST

보안 감사 보고서

FINAL

IOST 감사 보고서

Ver_1.0

SOOHO

www.sooho.io

1. 도입

1-1. 개요

아이오에스티(IOST)는 확장성과 빠른 트랜잭션 처리 속도에 집중하여 서비스의 인터넷(Internet of services, IOS)를 목표로 삼고 있는 블록체인 프로젝트입니다. 아이오에스티 토큰($IOST)은 아이오에스티 네트워크 내의 모든 트랜잭션 수수료 지불에 사용되고 있습니다. 아이오에스티는 합의 알고리즘으로 신뢰성증명 방식(Proof of Believability, PoB)을 사용하고 있습니다. 해당 알고리즘 하에서 네트워크 기여도가 높은 노드들의 무작위 추첨을 통해서 유효성 검증을 하며, 이를 통해 검증인 선출과정에서의 중앙화를 방지할 수 있습니다. 또한, 아이오에스티는 효율분산샤딩(Efficient Distributed Sharding, EDS) 방식을 통해 트랜잭션 속도를 대폭 개선하였습니다. 효율분산샤딩은 거래처리에 필요한 노드들을 그룹화시켜 처리하는 기술로서 높은 확장성과 효율성을 가집니다.

SOOHO Audit은 IOST에 대한 보안 감사를 **2023년 4월 25일에서 2023년 4월 28일의 4일간 진행**하였습니다. 이번 보안 감사는 IOST 메인넷을 대상으로, **다크코인 여부와 자금세탁 여부를 분석하는 것을 목적**으로 합니다.

본 감사에서 SOOHO Audit은 하기와 같은 시나리오에 대한 검토를 진행하였습니다:

[비식별화에 따른 불투명성]
- 블록체인 원장과 거래내역을 누구나 확인할 수 있는가
- OSS 기반의 노드 SW가 존재하고, 구동 시 모든 온체인 데이터 (트랜잭션, 유저 정보, 노드 등) 열람 가능한가?
- Block Explorer 서비스가 존재하는가? 구현이 가능한가?

[가상자산의 자금세탁 악용 가능성]
- 자산 별 자금 흐름 파악이 가능한가
- 계정 별 자금 흐름 파악이 가능한가
- 백서 내용과 다른 부분이 있는가

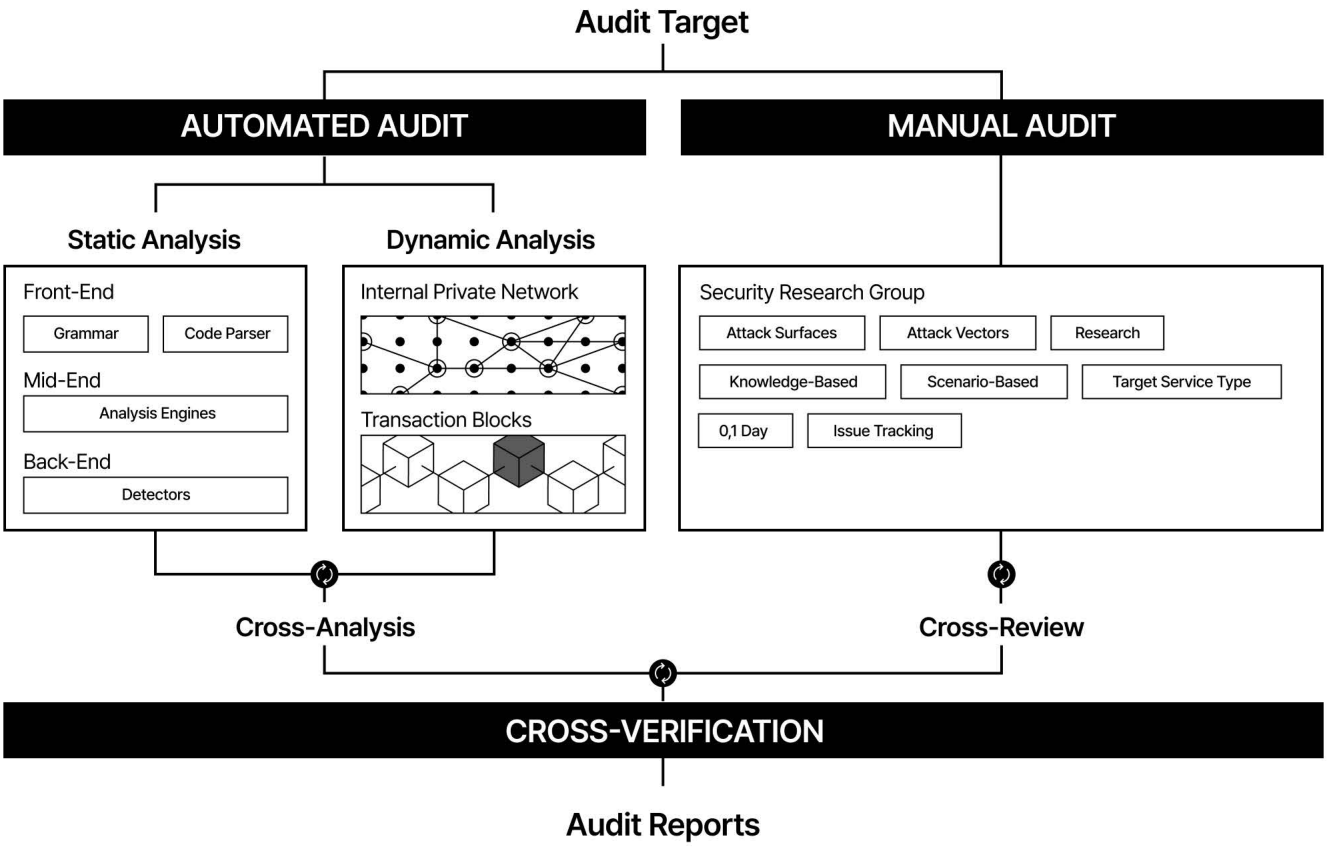
결과적으로, SOOHO Audit은 **문제점을 발견하지 못했습니다. 즉, IOST는 다크코인이 아니며, 자금세탁을 위한 블록체인이 아닙니다.** 본 감사를 통해 성공적으로 주요 가능성에 대한 검증을 하였지만, 본 감사가 주어진 자원 내에서 감사의 목표를 효율적으로 달성하기 위한 가장 필수적인 측면들에 국한한 검증을 수행하였다는 점을 알려드립니다. 지속적인 보안 감사를 통해 프로젝트의 안전성을 지속적으로 제고해 나가기를 권고드립니다.

1-2. 방법론

SOOHO Audit은 **자동 분석(Automated Audit)과 수동 분석(Manual Audit)의 두 가지 감사 방법론**을 적용하여 더욱 완벽한 블록체인 보안 감사를 진행합니다.

자동 분석은 **정적 분석(Static analysis)과 동적 분석(Dynamic analysis) 사이 상호 협력적 분석**을 통해 다양한 공격을 정확하고 빠르게 찾아내며 **높은 감사 퀄리티를 보장**합니다. SOOHO의 자체 분석기는 정적 분석을 통해 고객사 컨트랙트 코드의 문법을 분석(parsing)하여 의미 추론, 변수 추적, 경로 탐색을 진행함으로써 조건을 검증합니다. 정적 분석에서는 SOOHO 자체 테스트 네트워크에서 실제 동작을 통한 분석과 퍼징(Fuzzing), 콘콜릭 실행(Concolic Execution)을 통해 더욱 정교한 분석을 진행합니다.

수동 분석에서는 **SOOHO의 보안 감사 전문가 그룹**이 다양한 보안 및 도메인 지식을 활용하여 **고객사의 프로젝트를 직접 검증**합니다. 보다큰 리스크를 내포하는 코드를 중점적으로 분석하고, 파트너 사가 의도한 대로 코드가 작성되었는지 살피며 접근 권한의 관리가 올바르게 기능하고 있는지 검사합니다. 보안 감사 전문가들은 복잡한 공격 시나리오나 최근 보안 이슈를 처리하며 자동 분석을 상호 보완하여 감사의 완성도를 높입니다. 또한, 전문가 사이의 교차 검증을 통해 더욱 정교한 보안 감사 결과물을 제공합니다.



SOOHO.IO

수호아이오
보안 감사 인증서

SOOHO.IO Verified on Jan 4th, 2023

감사 대상

체인	아이오에스티	**구현 언어**	고(Go)
감사 대상 파일수	1,348,611		
검사 대상 저장소	https://github.com/iost-official/go-iost		
검사 기준 커밋	28501e14e9aec11e7afbfd9d9d9ddb07ec06151d		
검사 기간	2023년 4월 25일 - 2023년 4월 28일		

탐지된 이슈

탐지됨	해결됨	일부 해결됨	확인됨
0	0	0	0

CRITICAL	0
HIGH	0
MEDIUM	0
LOW	0
NOTE	0

2. 감사 요약

2-1. 탐지된 이슈 요약

문서 변경 기록 Ver_1.0 - 2023년 4월 28일 발행 : 최초 감사 보고서 전달

이슈 ID	심각도	이슈 상세	상태
-	-	-	-

2-2. 검증 내용 상세

검증 ID	검증 내용	검증 여부
Darkcoin	비식별화에 따른 불투명성이 없어야 합니다.	ⓒ 검증됨
AML	가상자산의 자금세탁 악용 가능성이 없어야 합니다.	ⓒ 검증됨

3. 분석 내용 상세

#1. 확인됨. 블록체인 원장과 거래내역을 누구나 확인할 수 있음

상태	✓ 검증됨
이슈 분류	Darkcoin

이슈 상세

본 프로젝트는 go-iost를 바탕으로 누구나 iost 원장에 접근하고 동일한 데이터를 확인할 수 있음이 확인되었습니다. 두 개 이상의 노드에서 sync를 한 블록데이터가 genesis부터 분석 시점까지 모두 동일한 데이터를 가지고 있음을 확인하였습니다. 이를 바탕으로 데이터에 대한 투명성을 확인하였습니다.

#2. 확인됨. OSS 기반의 노드 SW에서 모든 온체인 데이터 열람 가능

상태	✓ 검증됨
이슈 분류	Darkcoin

이슈 상세

본 프로젝트는 누구나 사용가능한 노드 SW가 오픈소스 소프트웨어 (OSS)로 구성되어 있습니다. 이를 바탕으로 모든 트랜잭션과 원장 정보를 동일하게 확인할 수 있음을 확인하였습니다.

#3. 확인됨. Block Explorer 서비스가 존재하는가? 구현이 가능한가?

상태	✓ 검증됨
이슈 분류	Darkcoin

이슈 상세

본 프로젝트는 누구나 사용가능한 블록 익스플로어 서비스가 존재하며, 오픈소스 소프트웨어 (OSS)로 구성되어 있습니다. 이를 바탕으로, 모든 트랜잭션과 원장 정보를 동일하게 확인할 수 있음을 확인하였습니다.

#4. 확인됨. 자산 별 자금 흐름 파악이 가능함

상태	✓ 검증됨
이슈 분류	AML

이슈 상세

노드 소프트웨어를 바탕으로, genesis 블록부터 현재까지 블록 생성 보상이 백서와 동일한지와 모든 자산이 특정 계정에 전송이 되거나 잔고(balance)로 표시되는지를 모두 확인하였습니다.

#5. 확인됨. 계정 별 자금 흐름 파악이 가능함

상태	✓ 검증됨
이슈 분류	AML

이슈 상세

노드 소프트웨어를 바탕으로, 계정 별 자산의 이동을 추적하였고 이를 바탕으로 트랜잭션의 실행 이후, 전송(from) 주소와 수신(to) 주소 간의 잔고(balance) 변화의 합이 0임을 genesis 블록부터 모두 확인하였습니다.

4. 부록

4-1. 심각도 정의

CRITICAL	**일반적인 상황에서** 명백하게 **자산의 직접적인 유출**이 발생하거나 시스템의 **즉각 중지**를 일으킬 수 있음
HIGH	**일반적인 상황**에서 명백하게 **자산의 간접적인 유출**이 발생하거나, 시스템이 **중지**될 수 있음
MEDIUM	자산의 유출이 일어나지는 않지만, 시스템의 **일시 정지**를 일으킬 수 있거나, 매우 특정한 상황에서 자산의 유출을 일으킬 수 있음
LOW	자산의 유출이 일어나지 않으며, 매우 특정한 상황에서 시스템의 일시정지를 일으킬 수 있거나, 기능 일부의 장애를 일으킬 수 있음
NOTE	시스템의 위협은 없으나, 기능적 최적화를 위해 권고됨

수호아이오 소개

SOOHO는 블록체인 생태계의 안전성과 신뢰도를 높이기 위한 기술을 연구하고 제공하고자 시작하였습니다. SOOHO는 자체적으로 개발한 취약점 분석기와 오픈 소스 분석기로 스마트 컨트랙트 취약점을 검증합니다. 더하여, SOOHO의 보안팀은 Defcon, Nuit du Hack, 화이트햇, SamsungCTF 등 국내외의 해킹 대회에서 수상하고, 보안분야 박사 학위와 같은 학문적 배경을 가지는 등 우수한 해킹 실력과 경험을 가진 보안 전문 인력들로 구성되어 있습니다. SOOHO의 전문 전문가들은 알려진 1-DAY 취약점부터 0-DAY 취약점으로부터 고객사의 스마트 컨트랙트를 보호하고자 합니다.

CONTACT US

Twitter	@SOOHO_AUDIT
E-mail	audit@sooho.io
Website	https://audit.sooho.io/

면책 조항

본 보고서는 서비스 계약에 명시된 약관(서비스 설명, 기밀 유지, 면책 및 책임 제한을 포함하되 이에 국한되지 않음) 또는 서비스 범위, 계약과 관련하여 귀하("고객" 또는 "회사")에게 제공되는 약관 및 조건의 적용을 받습니다. 본 계약에 명시된 서비스와 관련하여 제공되는 본 보고서는 본 계약에 명시된 약관에 따라 허용되는 범위 내에서만 회사가 사용할 수 있습니다. 본 보고서는 어떠한 목적으로도 회사 이외의 다른 사람에게 전송, 공개, 참조 또는 의존할 수 없으며, 각 경우에 SOOHO.IO의 사전 서면 동의 없이는 사본을 전달할 수 없습니다. 이 보고서는 특정 프로젝트 또는 팀을 "승인" 또는 "비승인"하는 것이 아니며, 그렇게 간주되어서도 안 됩니다. 이 보고서는 보안 평가를 수행하기 위해 SOOHO.IO와 계약을 맺은 팀 또는 프로젝트가 만든 "제품" 또는 "자산"의 경제성 또는 가치를 나타내는 것이 아니며, 그렇게 간주되어서도 안 됩니다. 이 보고서는 분석된 기술의 절대적인 버그 무결성에 대한 어떠한 보증이나 보장도 제공하지 않으며, 기술 소유자, 비즈니스, 비즈니스 모델 또는 법률 준수에 대한 어떠한 표시도 제공하지 않습니다. 이 보고서는 특정 프로젝트에 대한 투자 또는 참여와 관련된 결정을 내리는 데 어떠한 방식으로도 사용되어서는 안 됩니다.

이 보고서는 투자 조언을 제공하지 않으며, 어떤 종류의 투자 조언으로 활용되어서도 안 됩니다. 이 보고서는 고객이 코드의 품질을 높이는 동시에 암호화 토큰과 블록체인 기술로 인한 높은 수준의 위험을 줄이는 데 도움을 주기 위한 광범위한 평가 프로세스를 나타냅니다. 블록체인 기술 및 암호화 자산은 높은 수준의 지속적인 위험을 내포하고 있습니다. SOOHO.IO의 입장은 각 기업과 개인이 자체 실사와 지속적인 보안에 대한 책임이 있다는 것입니다. SOOHO.IO의 목표는 지속적으로 변화하는 새로운 기술 활용과 관련된 공격 벡터와 높은 수준의 편차를 줄이는 데 도움을 주는 것이며, 분석에 동의한 기술의 보안 또는 기능에 대한 어떠한 보장도 주장하지 않습니다. SOOHO.IO에서 제공하는 평가 서비스는 종속성에 따라 달라질 수 있으며 계속 개발 중입니다. 귀하는 서비스, 보고서 및 자료를 포함하되 이에 국한되지 않는 귀하의 액세스 및/또는 사용이 있는 그대로, 있는 그대로, 사용 가능한 대로 전적으로 귀하의 책임하에 이루어짐에 동의합니다. 암호화 토큰은 신흥 기술이며 높은 수준의 기술적 위험과 불확실성을 수반합니다. 평가 보고서에는 오탐, 오탐 및 기타 예측할 수 없는 결과가 포함될 수 있습니다.